Notice of Allowability	Application No.	Applicant(s)	
	10/036,196	HE ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *16 February 2007*.

2. ☒ The allowed claim(s) is/are *1-18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 8-16 have been amended.

2. Claims 1-18 are pending.

Response to Arguments

3. Applicant's arguments filed 16 February 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

4. **Claims 1-18** are allowed.

5. The following is an examiner's statement of reasons for allowance: The present invention is directed towards a method and system for internally encrypting data in a relational database. Claims 1 and 8 identifies the uniquely distinct features "**providing a database engine having encryption as a database kernel feature, providing a security dictionary comprising one or more security catalogs, receiving data from a user, associating said data with a database column and at least one authorized user, generating a working encryption key, internally encrypting said working encryption key within said database engine using a public key from an authorized user, storing said encrypted working key in a security catalog, and internally encrypting said data within said database engine using said working key**". Claim 17 identifies the uniquely distinct features "**fetching encrypted data pages from storage, computing a data encryption/decryption key, decrypting the data to form plaintext data pages, using said plaintext data pages, building an index and forming index pages, and encrypting said index pages**". Claim 18 identifies the

uniquely distinct features "**adding ENCRYPTION clause to a CREATE TABLE statement: adding USER clause to the CREATE TABLE statement, adding ENCRYPTION clause to an ALTER TABLE statement, adding KEY clause to an INSERT statement, adding KEY clause to a SELECT statement, adding UPDATE clause to a CREATE USER statement, and modifying core SQL statements to integrate encryption and key management as a core database feature supported internally by query compilation and execution components of a database system**". The closest prior art, Newman et al. (Pub No. 2003/0046572) discloses a transparent encryption infrastructure which allows the user to point-and-click on columns and tables to encrypt data. The creation of triggers and views are also easily implemented, to encrypt and decrypt data, to manage the encryption keys and to grant and revoke access to a column. Public and private key pairs are hashed and encrypted with a valid password. The process or encryption starts by creating a randomly generated symmetrical key, encrypting the symmetrical key with the private key for each user authorized to decrypt the data, and storing the encrypted symmetrical key, along with the user's name and the column name, in the database. These cryptosystems allow a user to digitally encrypt information stored in a non-relational format such as flat files residing on an operating system. This is accomplished by encrypting and decrypting the entire non-relational file with a single encryption key and storing that single encryption key offline in a secure format. However, either singularly or in combination, Newman et al. fail to anticipate or render the claimed limitation of providing a database engine having encryption as a database kernel feature, providing a security dictionary

comprising one or more security catalogs, receiving data from a user, associating said data with a database column and at least one authorized user, generating a working encryption key, internally encrypting said working encryption key within said database engine using a public key from an authorized user, storing said encrypted working key in a security catalog, and internally encrypting said data within said database engine using said working key. The closest prior art, Harashima et al. (JP Pub No. 2003/271438) discloses a program, system, and method for preventing contents of individual data from being grasped and realize sufficient data protection while admitting access right necessary for operation and management of a database to a database manager. However, either singularly or in combination, Harashima et al. fail to anticipate or render the claimed limitation of providing a database engine having encryption as a database kernel feature, providing a security dictionary comprising one or more security catalogs, receiving data from a user, associating said data with a database column and at least one authorized user, generating a working encryption key, internally encrypting said working encryption key within said database engine using a public key from an authorized user, storing said encrypted working key in a security catalog, and internally encrypting said data within said database engine using said working key.

The closest prior art, I. Wassim, A. Kayssi, and A. Chehab, "An enterprise policy-based security protocol for protecting relational database network objects" discloses an enterprise policy-based security protocol for protecting relational database network objects for ensuring the confidentiality and integrity of database objects flowing over network links between the enterprise information system layer represented mainly in

relational database servers. However, either singularly or in combination, I. Wassim, A. Kayssi, and A. Chehab fail to anticipate or render the claimed limitation of providing a database engine having encryption as a database kernel feature, providing a security dictionary comprising one or more security catalogs, receiving data from a user, associating said data with a database column and at least one authorized user, generating a working encryption key, internally encrypting said working encryption key within said database engine using a public key from an authorized user, storing said encrypted working key in a security catalog, and internally encrypting said data within said database engine using said working key.

6. Therefore, **claims 1,8,17, and 18**, and the respective **dependent claims 2-7 and 9-16** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
May 2, 2007

MATTHEW SMITHE
PRIMARY EXAMINE
Art Unit 2137